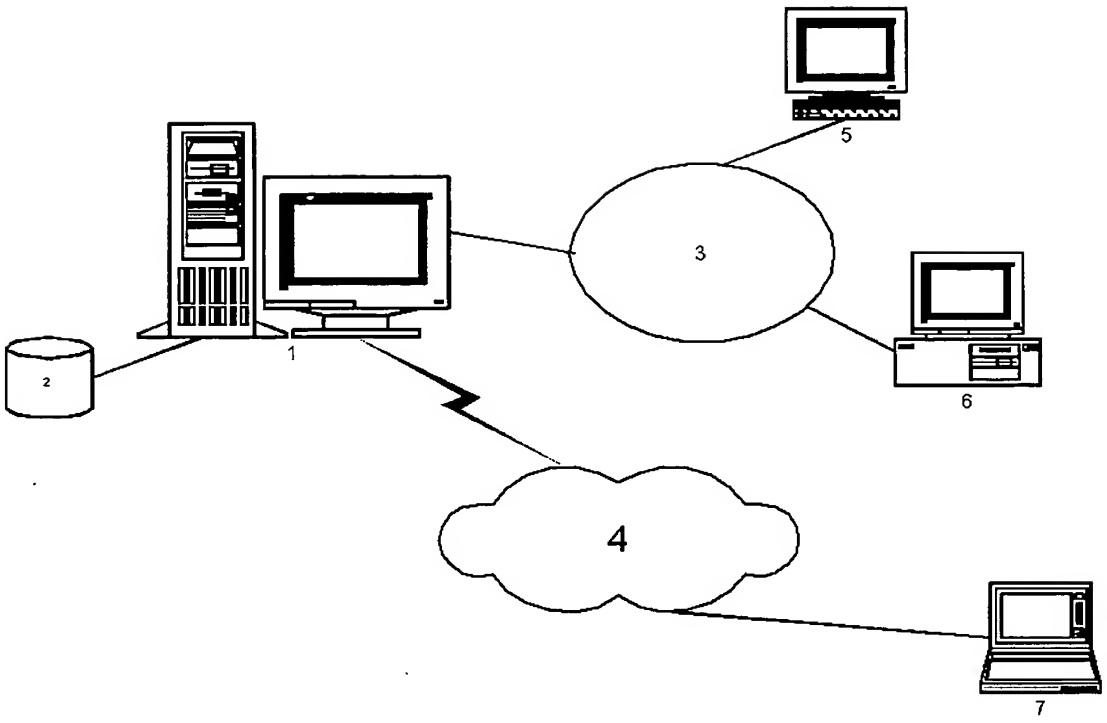


Figure 1

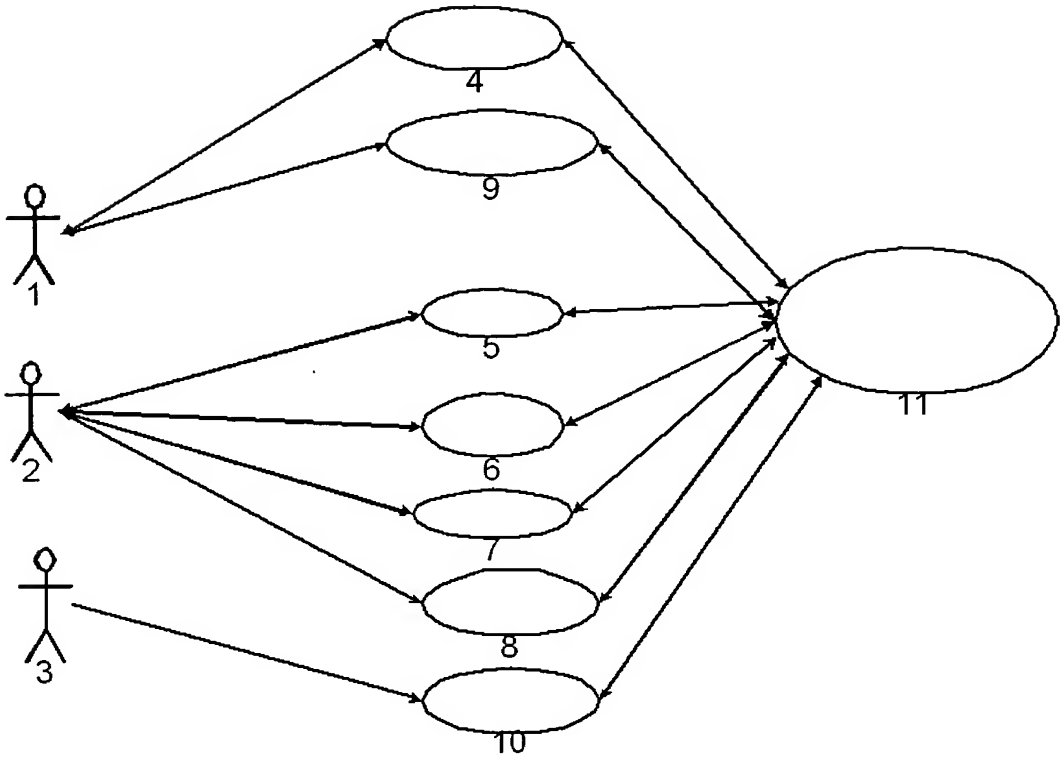


Figure 2

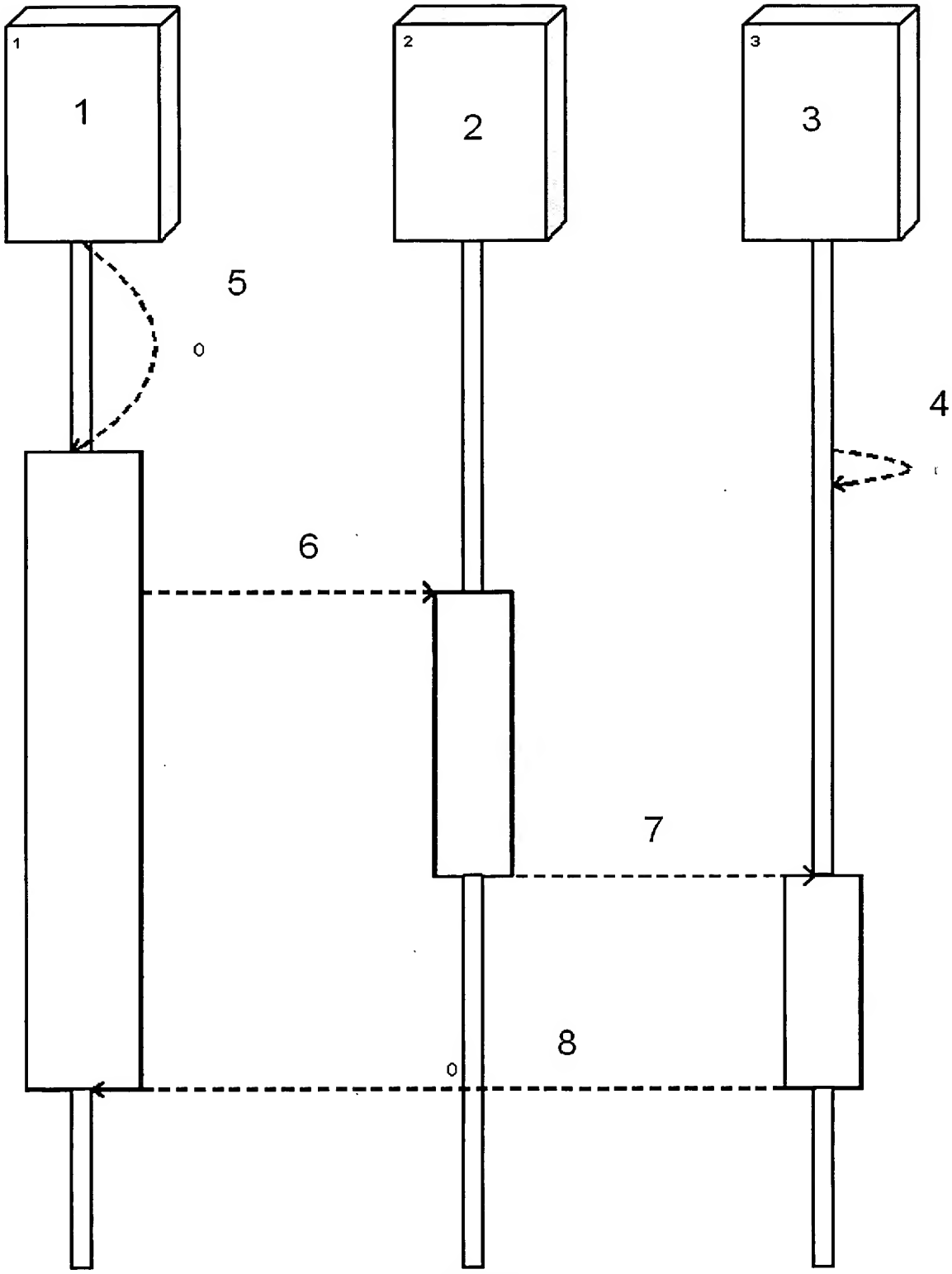


Figure 3

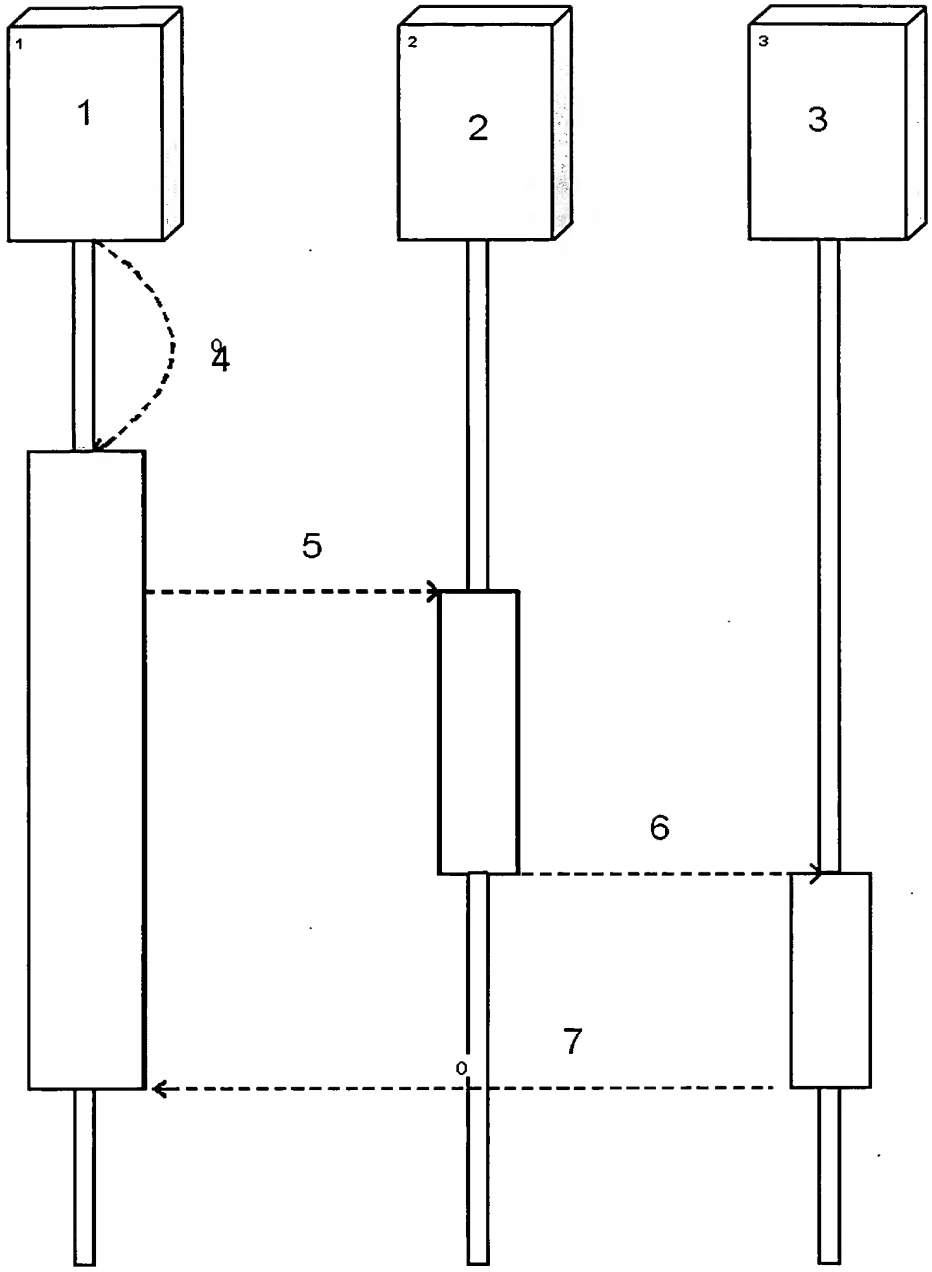
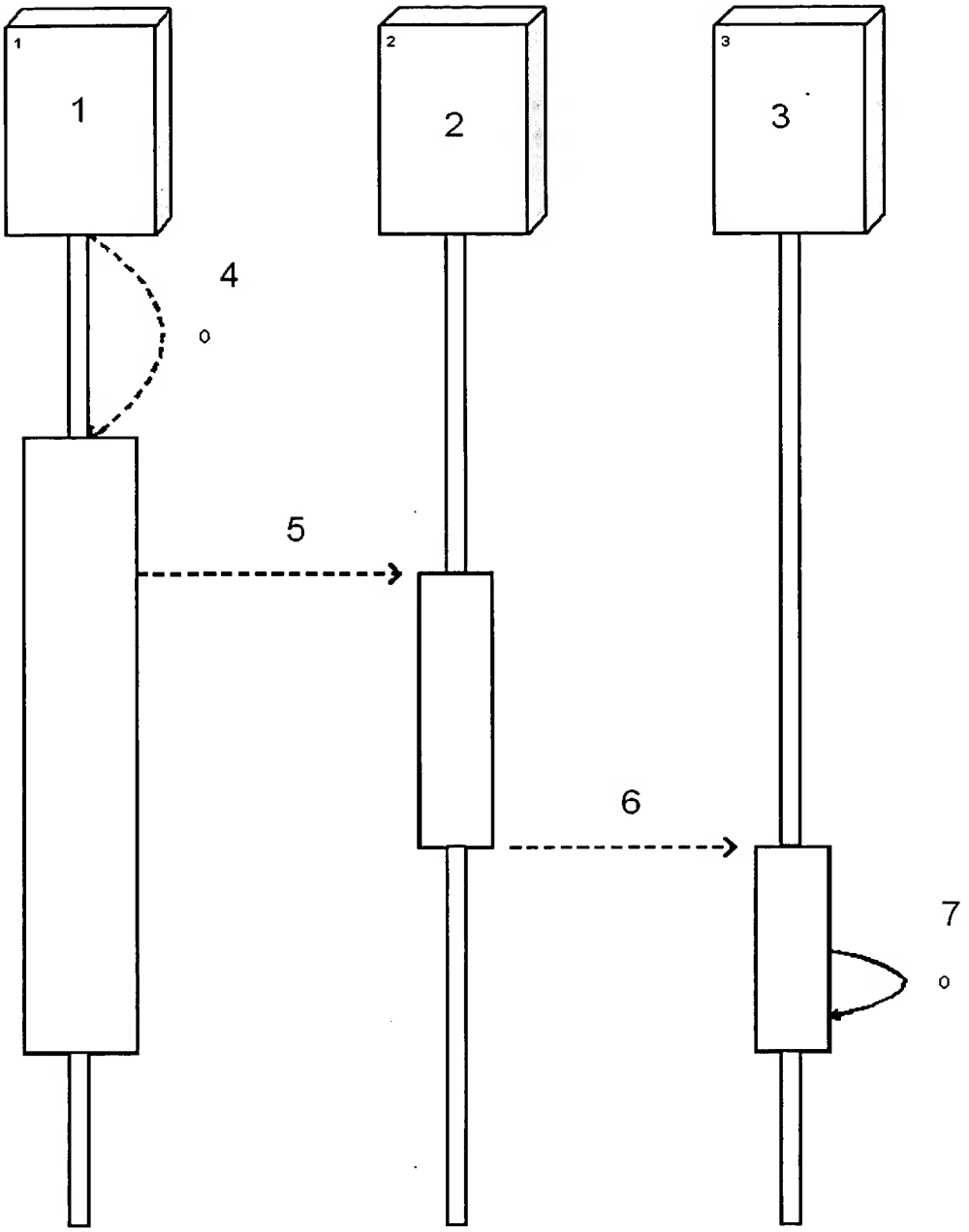


Figure 4



5

Figure 5

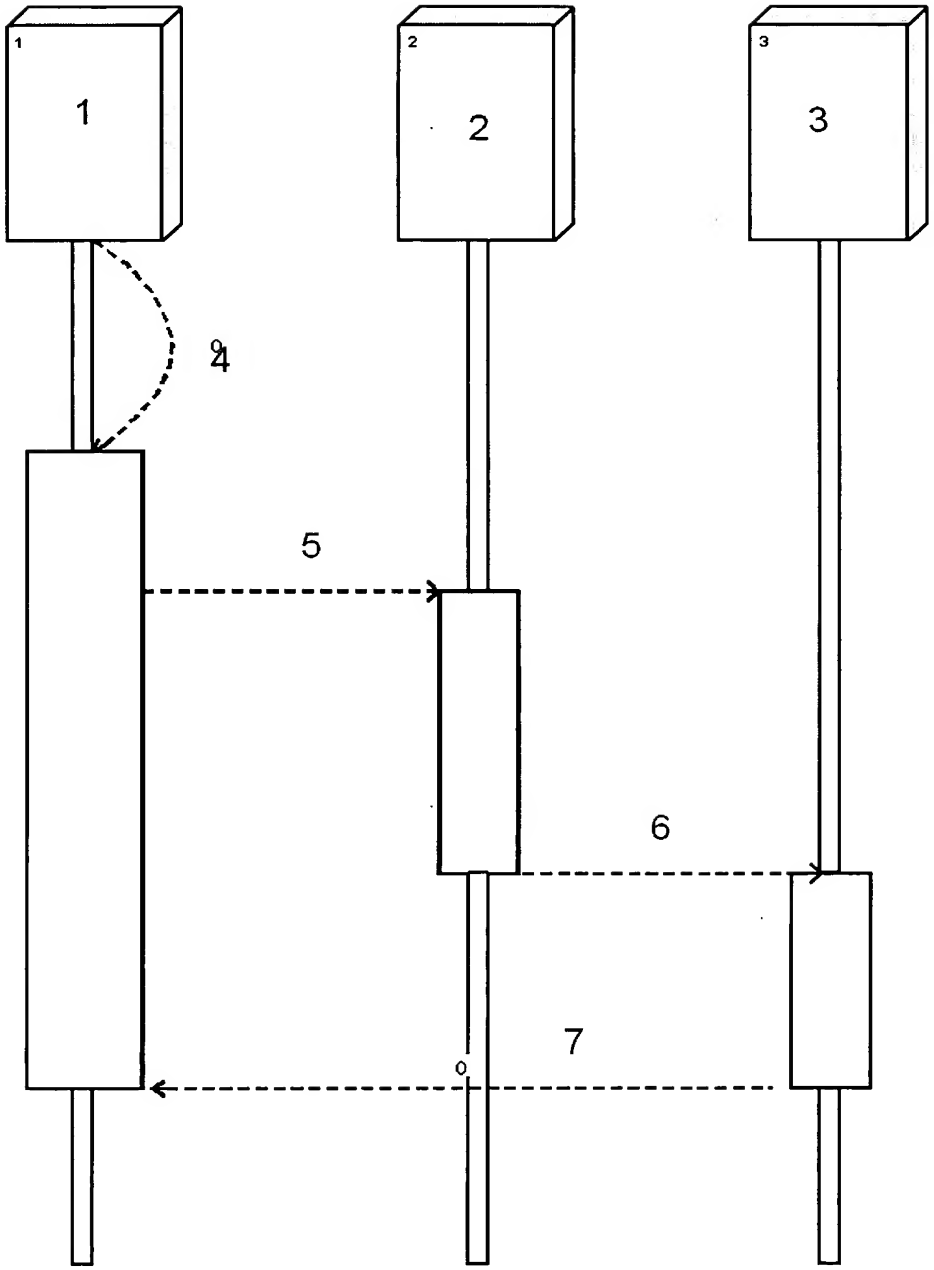


Figure 6

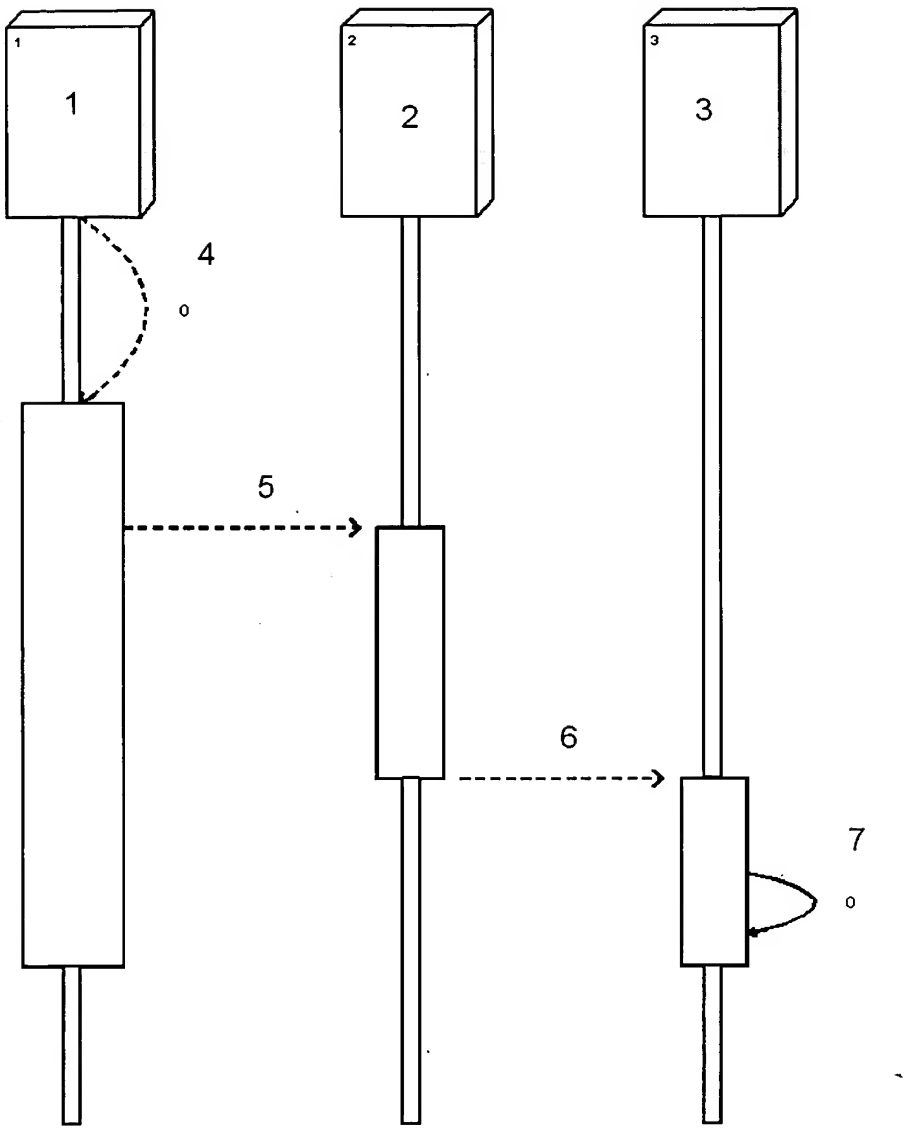


Figure 7

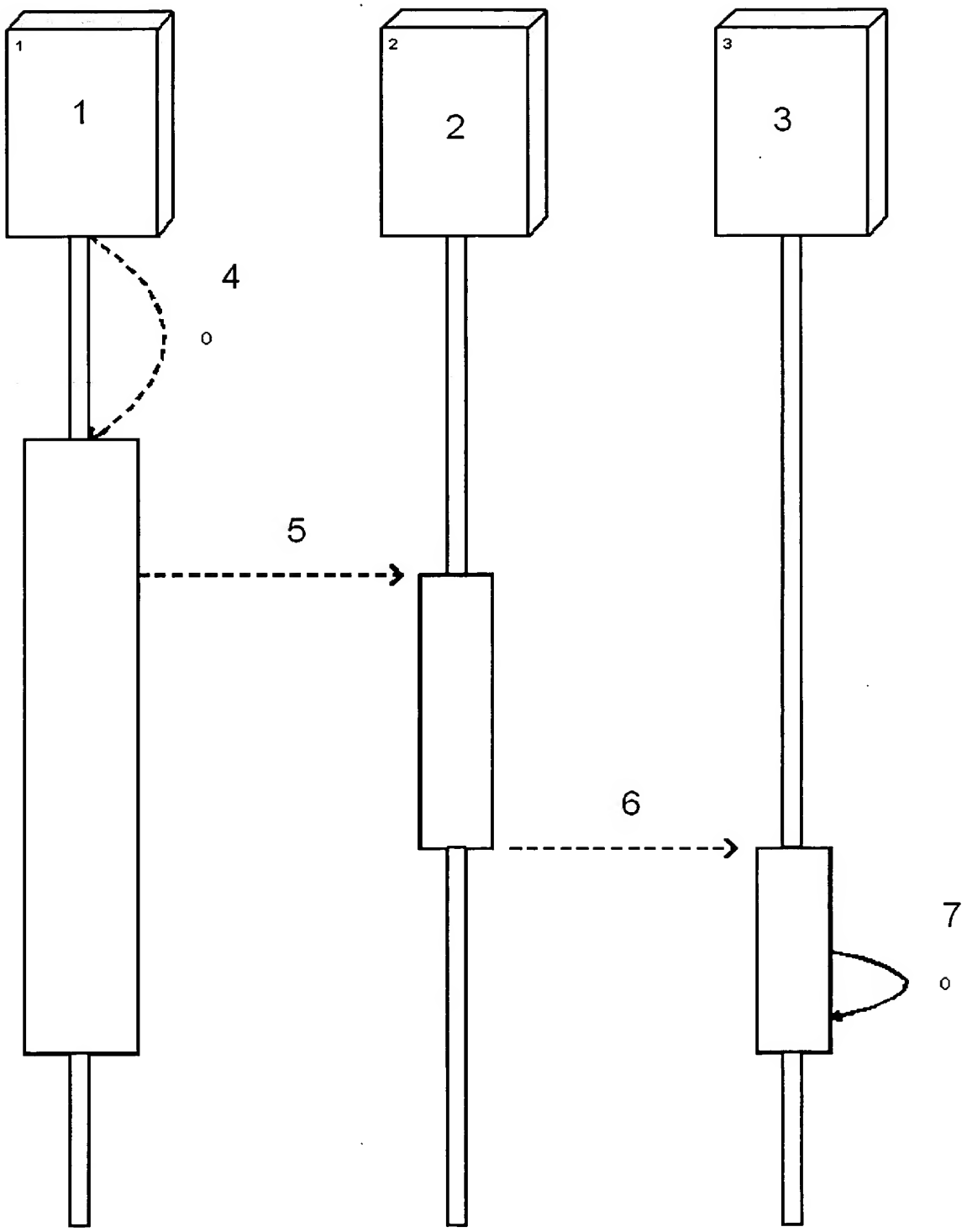


Figure 8

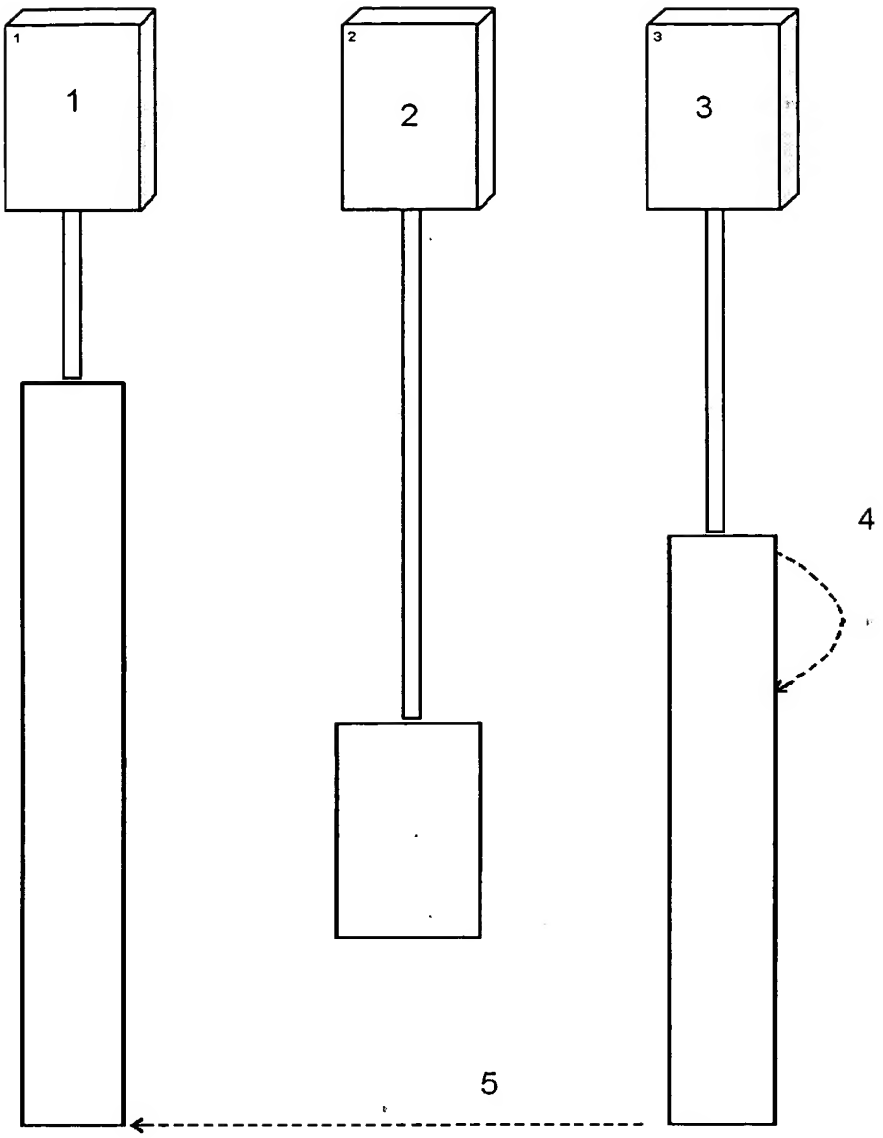


Figure 9

5

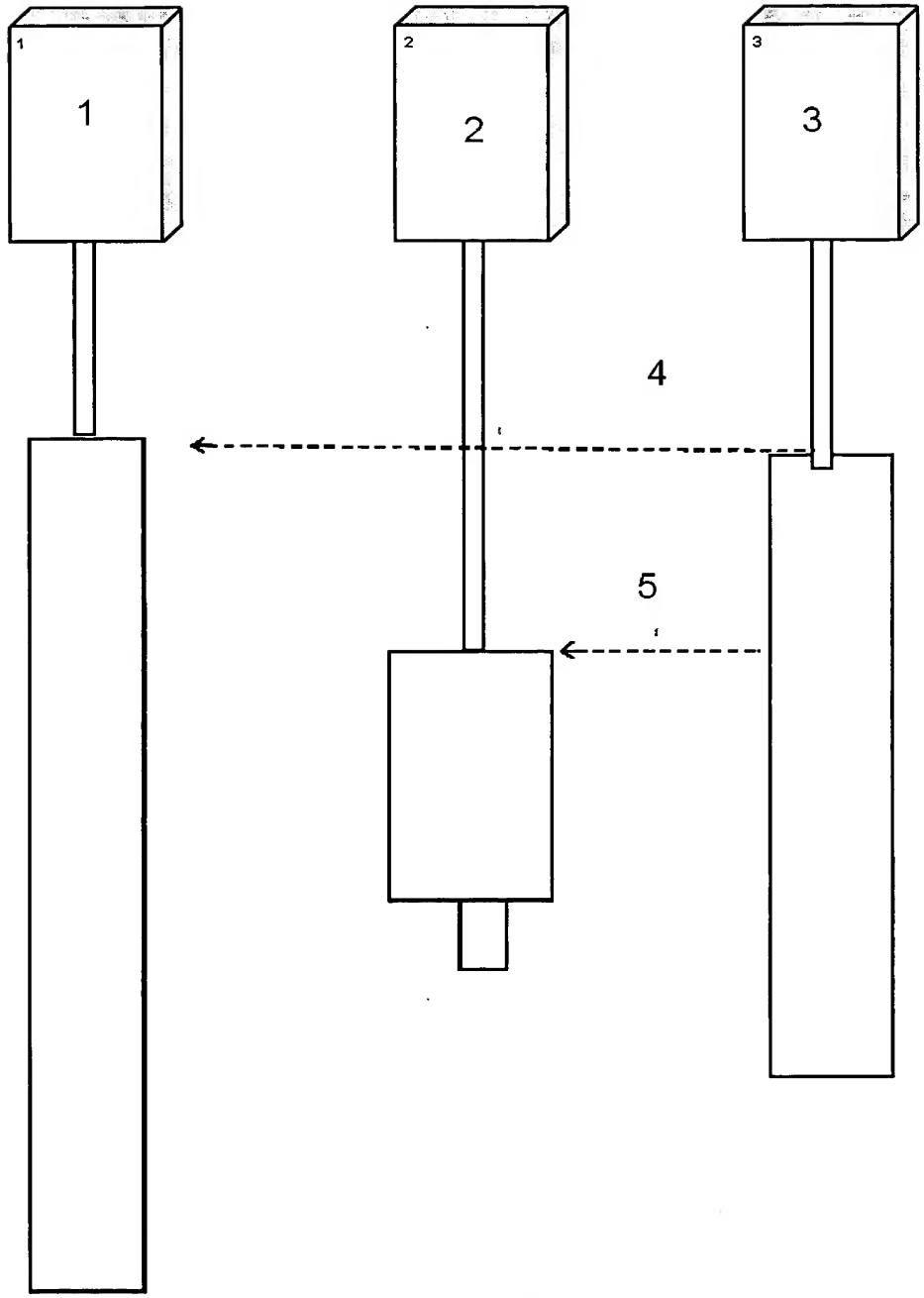


Figure 10

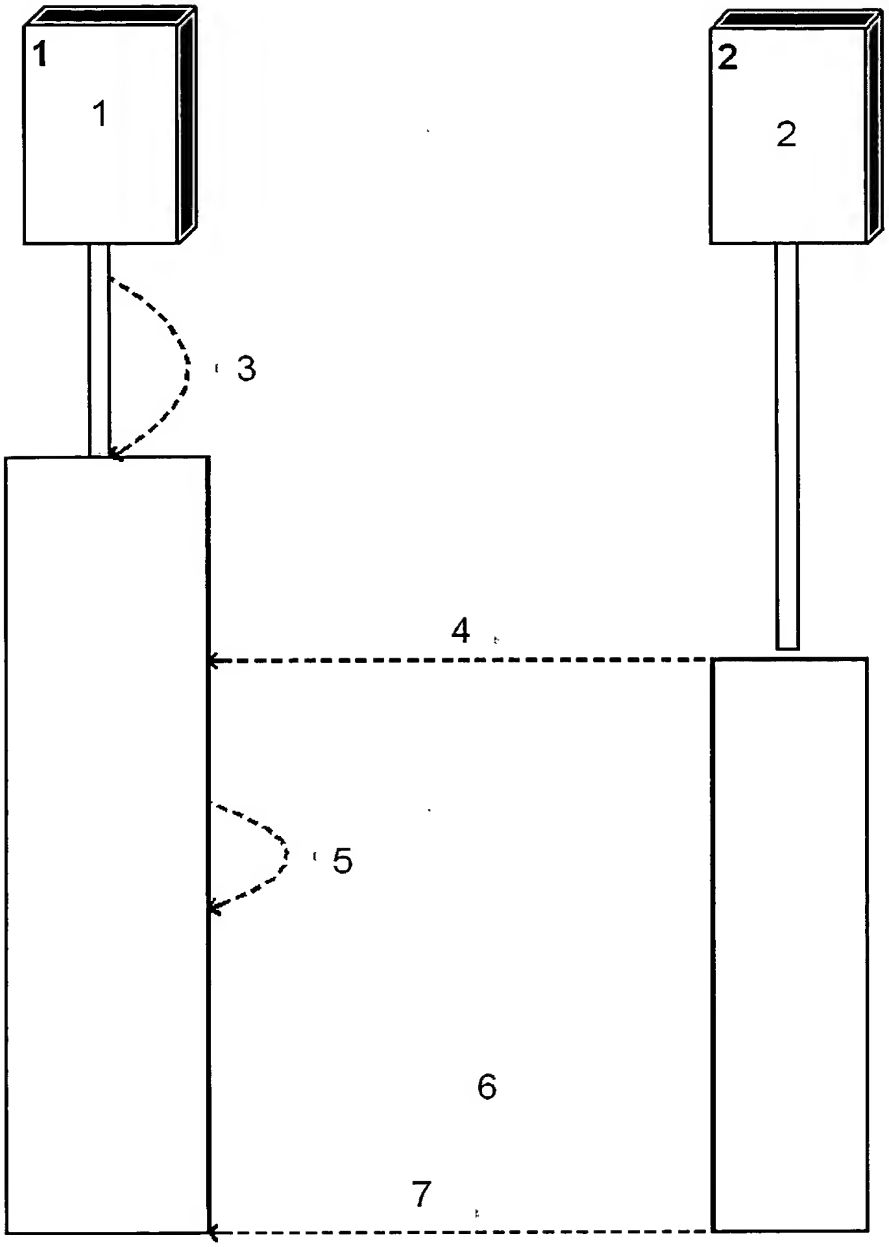


Figure 11

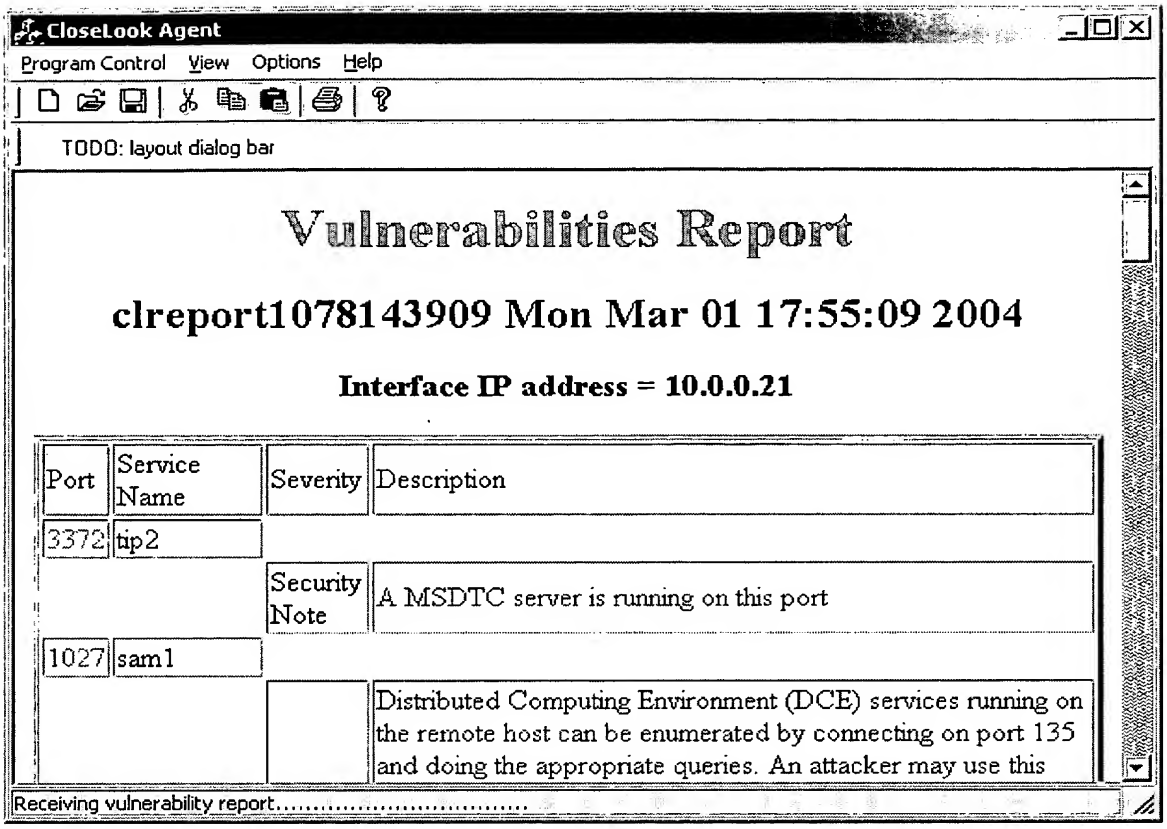

CloseLook Agent
Program Control View Options Help
TODO: layout dialog bar
Vulnerabilities Report
clreport1078143909 Mon Mar 01 17:55:09 2004
Interface IP address = 10.0.0.21
Port
Service Name
Severity
Description
3372
tip2
Security Note
A MSDTC server is running on this port
1027
sam1
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this
Receiving vulnerability report.....

Figure. 12

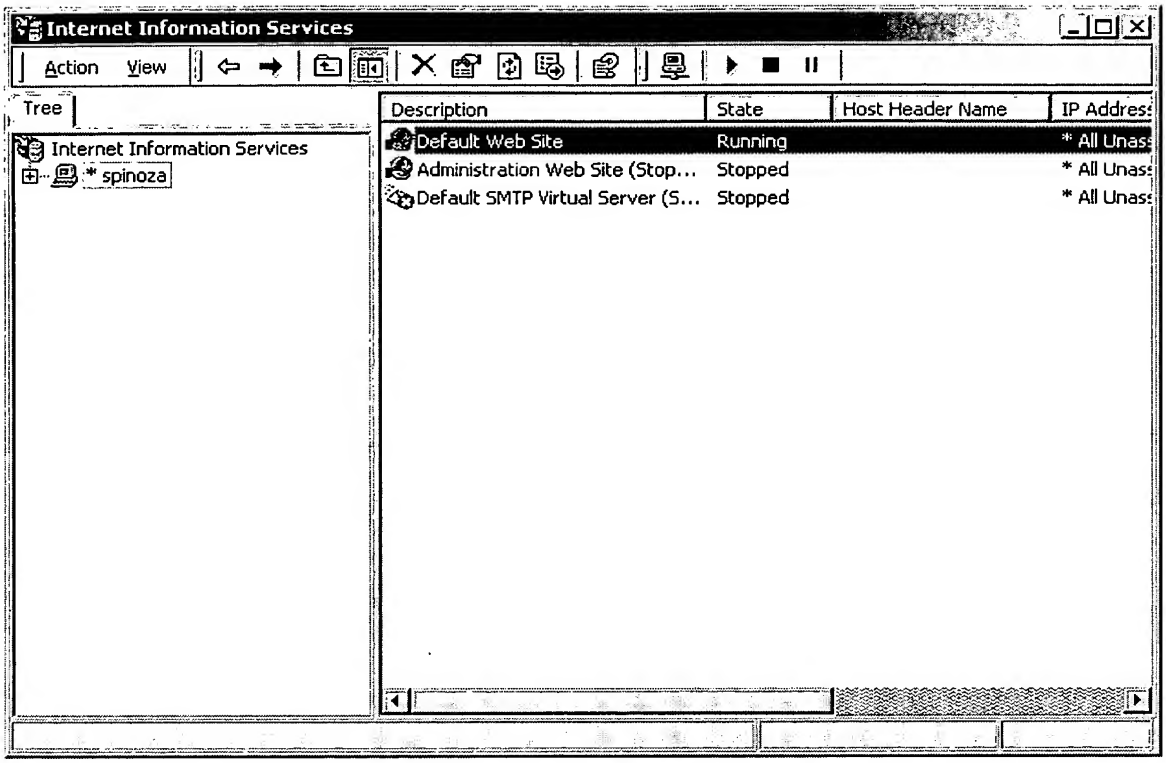

Internet Information Services
Action
View
Tree
Internet Information Services
* spinoza
Description
State
Host Header Name
IP Addres
Default Web Site
Running
* All Unas
Administration Web Site (Stop...
Stopped
* All Unas
Default SMTP Virtual Server (S...
Stopped
* All Unas

Figure. 13

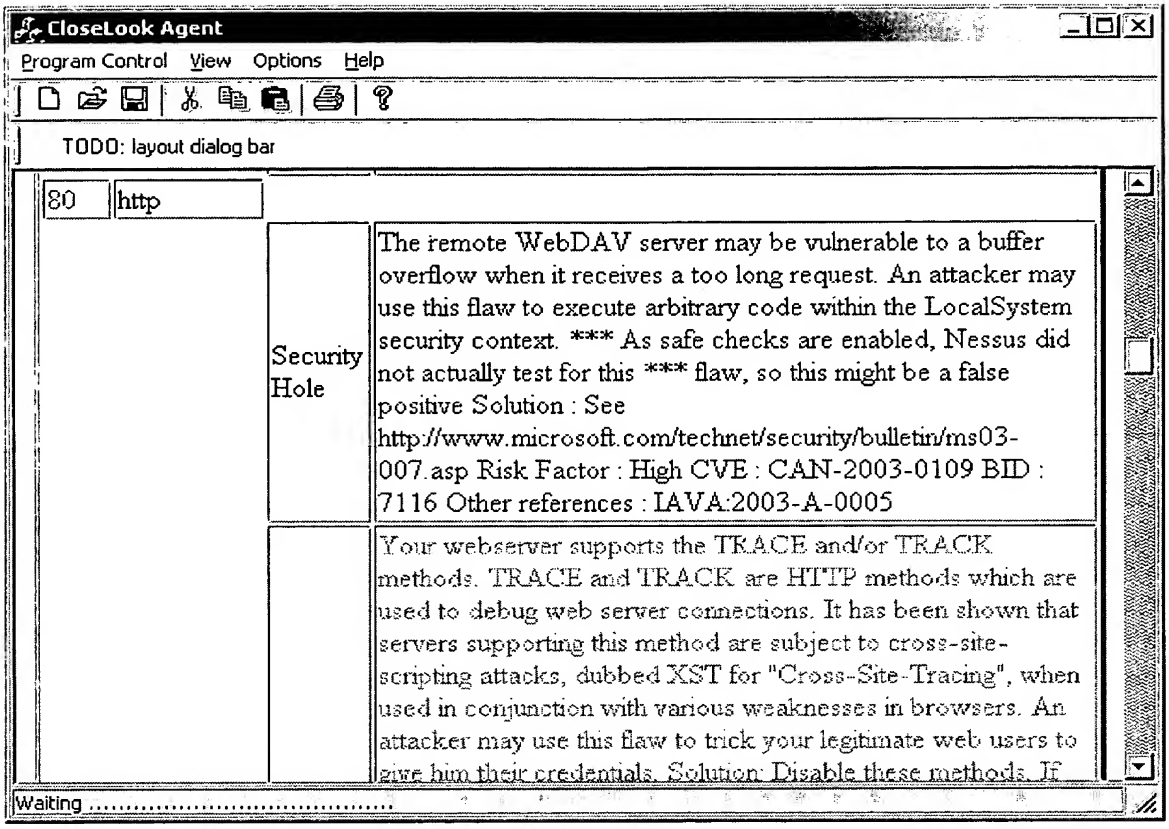

CloseLook Agent
Program Control View Options Help
TODO: layout dialog bar
80
http
Security Hole
The remote WebDAV server may be vulnerable to a buffer overflow when it receives a too long request. An attacker may use this flaw to execute arbitrary code within the LocalSystem security context. *** As safe checks are enabled, Nessus did not actually test for this *** flaw, so this might be a false positive Solution : See http://www.microsoft.com/technet/security/bulletin/ms03-007.asp Risk Factor : High CVE : CAN-2003-0109 BID : 7116 Other references : IAVA:2003-A-0005
Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution: Disable these methods. If
Waiting .....

Figure. 14

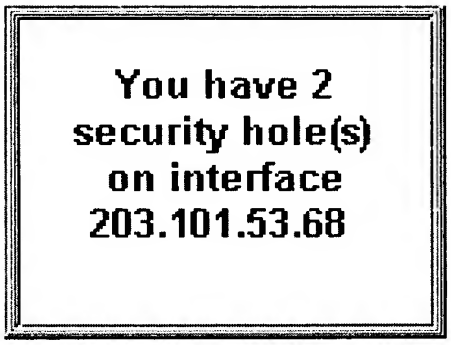


Figure. 15